WLD1993004 WO 9301550 A1 930121

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 11/34, H04L 9/00

A1

(11) International Publication Number: WO 93/01550

(43) International Publication Date: 21 January 1993 (21.01.93)

(21) International Application Number: PCT/US92/05387

(22) International Filing Date: 30 June 1992 (30.06.92)

(30) Priority data:

724,180	1 July 1991 (01.07.91)	US
907,934	29 June 1992 (29.06.92)	US

(71) Applicant: INFOLOGIC SOFTWARE, INC. [US/US]; 1223 Peoples Avenue, Suite 5405, Troy, NY 12180 (US).

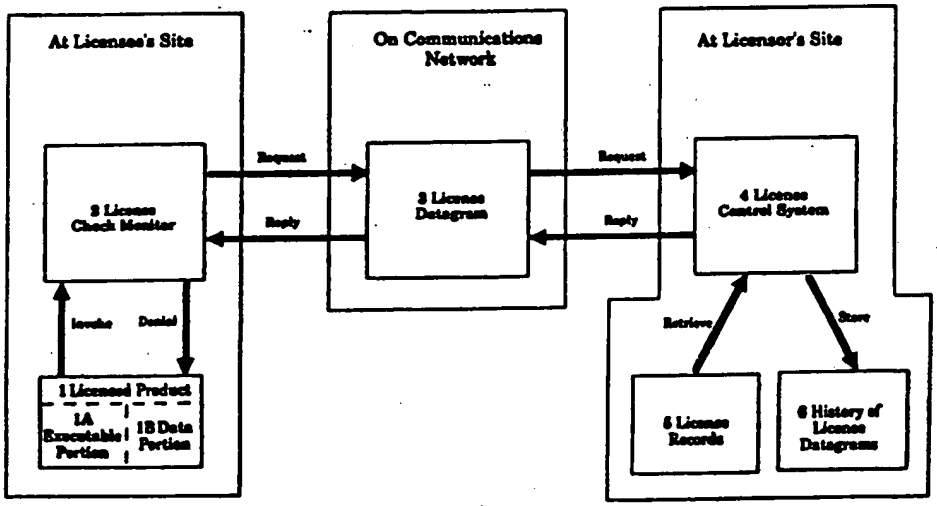
(72) Inventor: GRISWOLD, Gary, N. ; 1937 Regent Street, Schenectady, NY 12309 (US).

(74) Agents: LAZAR, Dale, S. et al.; Cushman, Darby & Cushman, Ninth Floor, 1100 New York Avenue, N.W., Washington, DC 20005-3918 (US).

(81) Designated States: AT, AU, BB, BG, BR, CA, CH, CS, DE, DK, ES, FI, GB, HU, JP, KP, KR, LK, LU, MG, MN, MW, NL, NO, PL, RO, RU, SD, SE, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, MC, NL, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, SN, TD, TG).

Published
With international search report.

(54) Title: LICENSE MANAGEMENT SYSTEM AND METHOD



(57) Abstract

A license management system and method for recording (6) the use of licensed product (1), and for controlling (4) its use. A licensed product invokes a license check monitor (2) at regular time intervals. The monitor generates request datagrams (3) which identifiy the licensee and the product and sends the request datagrams over a communicati ns facility to a license control system (4). The license control system maintains a record (6) f the received datagrams, and compares the received datagrams to data stored in its licensee database (5). C nsequently, the license control system (4) transmits reply datagrams with either a denial r an approval message. The monitor (2) generates its own denial message if its request datagrams are unanswered after a prede-

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	ML	Mali
AU	Australia	FR	France	MN	Mongolia
BB	Barbados	GA	Gabon	MR	Mauritania
BE	Belgium	GB	United Kingdom	MW	Malawi
BF	Burkina Faso	GN	Guinea	NL	Netherlands
BG	Bulgaria	GR	Greece	NO	Norway
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IE	Ireland	RO	Romania
CA	Canada	IT	Italy	RU	Russian Federation
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CI	Côte d'Ivoire	LI	Liechtenstein	SU	Soviet Union
CM	Cameroon	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
DE	Germany	MC	Monaco	US	United States of America
DK	Denmark	MG	Madagascar		
ES	Spain				

LICENSE MANAGEMENT SYSTEM AND METHOD

BACKGROUND

Field of the Invention

The present invention generally relates to systems for managing licenses of products such as computer software, video games, CD-ROM information, movies and other video products, music and other audio products, multimedia products, and other systems for up-to-date recording of actual usage of such a licensed product to enable efficient billing therefor.

Description of Related Art

Licenses for information products such as computer software, music, video products and the like usually provide licensees with limited rights. The licenses may restrict sites of use, duration of use, or number of concurrent uses of the products. Th licenses also may limit the use of the products depending on currentness of licensee's payments. However, enforcing the conditions of the licenses is difficult, because, in general, the licensed products may be easily copied or "pirated" and used without the licensor's knowledge.

Compliance with limited license rights has been encouraged with copy protection. Known methods of computer software copy protection include putting a

physical hole or mark n the diskett containing a product, r placing data on the disk tt in a location where no data is expected. A disk with an illegally copied software product usually would not contain the marks. At the beginning of its operation, a copy-protected, but illegally copied software product would search its own diskette for the marks. Upon failing to detect the marks, the software would abort from its normal procedures.

Most software products sold today do not have such copy protection, partly because copy protection renders legitimate duplication of copy protected software difficult, but not impossible. Copy protection frustrates the making of legitimate copies, while not eliminating unauthorized copying. Many software publishers have experienced higher sales by eliminating copy protection schemes.

Another method for enforcing limited licensing rights of computer software is described in U.S. patent No. 4,932,054 to Chou. Chou describes a "coded filter" hardware device which is plugged into a port of a computer. The "coded filter" outputs an authorization control code when a predetermined control code is sent to it. The licensed software functions properly only if the "coded filter" transmits the correct authorization control code to the software.

While devices such as described by Chou hav existed for several years, they have not been well accepted by the market. Since the device is attach d to the outside of a computer, it can easily be lost or stol n, pr venting th us of licensed software. In addition, if a license purchas d a number of softwar

products, each of which used Chou's protection scheme, the licensee would collect a stack of "coded filters."

Hershey, in U.S. patent No. 4,924,378, describes a method for limiting the number of concurrent uses of a licensed software product. Each workstation of a network has a license storage area in its local memory. License Management System (LMS) daemons are provided in the network in a number corresponding to the permissible number of concurrent uses of the software product. To use the software, a work station stores a daemon in its license storage area. If all daemons are in use, no further work stations may use the software.

Robert et al., in U.S. patent No. 4,937,863, describe a similar invention. This invention includes a license management facility which accesses a database of license information related to licensed computer software programs. When a user attempts to use a licensed program, the license management facility first checks the database. Access to the licensed product is prevented if licensing conditions related to the product are not satisfied (e.g., expiration of licensing dates, etc).

While the Robert et al. and Hershey patents show effective techniques for controlling licensed computer software, each also reveals components that cannot be easily managed by an average user. A system manager, or someone with special access privileges to the internals of a machine, must install the licensed software. This hinders the distribution of the software.

Licensable products other than computer software have not generally been copy-protected. For example,

video tapes can be easily copied by anyone with two VCR machines, and audio tapes and music CDs can be easily copied to tape. Computer CD-ROMs can be copied to magnetic disk; however, their large information storage capacity relative to that of magnetic disks makes this a very expensive proposition. The introduction of digital audio tape is being delayed, because some view its ability to easily produce very high quality copies as a threat to music royalties.

Hellman, in U.S. patent No. 4,658,093, describes means to bill by usage. This is accomplished via communication of an encrypted authorization code from a licensor to a base unit at the licensee's site. The encrypted authorization code contains information related to an identification of the base unit, a number of uses requested, and a random or non-repeating number; however, implementation of Hellman's scheme requires a "base unit", such as a computer, video game unit, record player, video recorder, or video disk player, with a unique identification number. The requirement is difficult to satisfy, because, at the present, only a fraction of such systems on the market have an internally readable serial number for identification. In addition, vendors of these systems provide no guarantees for the uniqueness of any given device's serial number. Furthermore, an internal serial number can change when hardware maintenance is performed on the device. Also, Hellman's approach requires that an identical copy of each software product be stored at the authorization site. These copies are used in the generation of unique keys. The unstated assumption that all copies of a specific version of a software

product ar id ntical is unr alistic. Minor bug fixes t s ftwar ar oft n mad without gen rating a n w version of the product. Also, some s ftwar products, such as those which run on Macintosh computers, are self-modifying.

While Hellman's invention counts each use of the software, it does not monitor the duration of us . Thus, Hellman's system would not be able to bill for extensive use of licensed software if the softwar were continuously operated. Finally, while Hellman suggests the inclusion of an automated communication system as part of his invention, he does not disclose how this communication system could be implemented. Instead, he mentions non-automated use of telephone and mail. In summary, Hellman's patent is an interesting discussion of cryptographic techniques, but it does not provide a practical, real-world implementation of those techniques.

Shear, in U.S. Patent No. 4,977,594, describes a system and method to meter usage of distributed databases such as CD-ROM systems. The method describes a hardware module which must be part of th computer used to access the distributed databas . This module retains records of the information viewed. Once the module storage is filled, the module must be removed and delivered to someone who will charge for the usage recorded therein and set the module back to zero usage. Like Hellman's method, this method requires a hardware module which must be incorporated within the computer so the system can control user access. No database publisher will be able to us this method until there are a very large number of units containing such modules. Hardware manufacturers

will be hesitant to include the modul in the design of their computers until there is sufficient demand from customers or publishers for this system. The method and apparatus according to the present invention can be implemented entirely in software and hence does not require special, dedicated computer subsystems.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a license management system and method which can ensure that a licensed product is used only on machines under which it is licensed.

It is another object of the present invention to provide a license management system and method which may terminate access to a licensed product once its license has expired.

It is yet another object of the present invention to provide a license management system and method which may terminate access to a licensed product when payment for a license is overdue.

It is a further object of the present invention to provide a license management system and method which can limit the number of concurrent uses of a licensed product.

It is yet another object of the present invention to provide a license management system and method which can bill licensees for the duration of actual usage of a licensed product.

The present invention provides an advantageous feature of quickly and effectively implementing licensing agreements between a licensor and licensee.

The present invention provides another advantageous feature of allowing logic used to control licenses to be easily changed.

The present invention provides yet another advantageous feature of detecting, at the licensor's site, many types of attempts to alter the license management system.

The present invention provides a further advantageous feature of permitting anyone without special access privileges to install a licensed product.

In the present invention, a licensed product generates request "datagrams," messages transmitted over a communications network. The request datagrams are sent to the licensor's site. At the licensor's site the datagram is compared to information stored in a license database. After the comparison, a reply datagram is sent to the licensee. Upon receiving the reply datagram, the licensed product reacts in accordance with the instructions therewithin. For example if a reply datagram contained a "denial," the licensed product would display an appropriate message to the user and then suspend further execution of its programs.

In the present invention, the licensed product is implemented on a network node attached to a communications network that includes the licensor. The network node may be a computer, a CD-ROM player, a tele-computer or other multimedia machine, or any other appropriate device. The node may also be an intelligent type of consumer electronic device used for presenting information, such as an intelligent television, VCR, videodisk player, music CD player,

audi tap player, t l phon or other similar d vic . Furth r, th communications network may be any tw - way network such as a computer network, telephone network, a cellular telephone network or other wireless network, a two-way cable TV network, or any other equivalent system.

Should the user detach the node from the network, the licensed product will fail to receive reply datagrams. Upon several failures to receive reply datagrams, the licensed product will generate its own denial.

After a request datagram has been sent out, a user may be permitted to use the licensed product for a limited duration. This feature may be necessary because of the delays in network communications. When networks are sufficiently fast, use of a licensed product can be postponed until the reply datagram is received.

In the preferred embodiment of the present invention, licensees' network addresses are used to identify the licensees. Other embodiments may use a licensed product serial number or hardware serial numbers for the identification.

A licensed product as in the present invention generates a request datagram after each period of product use. The number of request datagrams received by the licensor can be used to bill the licensee. For example, if datagrams are sent after every hour of product use, the licensee will be billed for th amount equal to the number of request datagrams received by the licensor multiplied by the hourly rat .

The embodiments of the present invention may incorporate a query system at a licensor's site for reporting on problem datagrams. This would allow the licensors to take appropriate actions in accordance with problems associated with each datagram.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of this invention will become more apparent and more readily appreciated from the following detailed description of the presently preferred exemplary embodiment of the invention, taken in conjunction with the accompanying drawings, of which:

FIGURE 1 is a general block diagram of the preferred exemplary embodiment of the present invention;

FIGURE 2 shows representative diagrams of the contents and formats of data at licensee's site, contained in datagrams, and at licensor's site;

FIGURE 3 illustrates a sequence of representative operations executed at the licensee's site and at the licensor's site, together with required inputs for the execution of the operations and with outputs produced therefrom;

FIGURE 4 illustrates a sequence of representative operations to send a request datagram, together with required inputs for the execution of the operations and with outputs produced therefrom;

FIGURE 5 illustrates a sequence of representative operations when a reply datagram is overdue, together with required inputs for the execution of the operations and with outputs produced therefrom;

FIGURE 6 shows a sequence of representative operations to process a reply datagram, together with required inputs for the execution of the operations and with outputs produced therefrom;

FIGURE 7 shows a sequence of representative operations to generate an authorization code, together with required inputs for the execution of the operations and with outputs produced therefrom; and

FIGURE 8 shows a sequence of representative operations to send a reply datagram, together with required inputs for the execution of the operations and with outputs produced therefrom.

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EXEMPLARY EMBODIMENT

As shown in FIGURE 1, a licensed product 1 is located at a licensee's site. Product 1 may include a data portion 1B and a functional portion 1A such as computer software product or any other kind of information product used to control use of data portion 1B. If data portion 1B is CD-ROM database information, functional portion 1A should enable the licensee to search indexes and display text. If data portion 1B is video information, functional portion 1A should control the display of the video information. For audio information, functional portion 1A should play the audio information. If data portion 1B is an electronic book, functional portion 1A should display and turn pages. The above examples show some of the ways functional portion 1A can control data portion 1B; however, they are hardly exhaustive.

By including in product 1 both information and software which controls the information, product 1 is

an executable product. Non-software information in product 1 is preferably encrypted so that it cannot be easily extracted from the product.

License check monitor 2 sends license datagrams 3 to the licensor and also receives license datagrams 3 from the licensor. License check monitor 2 also prevents further use of product 1 when a datagram 3 containing a "denial" message is received.

License datagrams 3 are messages that describe information related to the use of licensed product 1. Datagrams 3 are sent over a communications network between the licensee and licensor. Initially, the licensee sends a request datagram 3 over the network to the licensor. The licensor then returns a reply datagram containing either an approval or denial. It is also possible to implement the present invention by having the licensor transmit a reply datagram only for approvals.

At the licensor's site, license control system 4 makes licensing decisions by comparing request datagram 3 with license records 5. After the comparison, control system 4 stores information related to request datagram 3 into history of license datagram record 6. It is noted that request datagrams 3 are periodically sent while product 1 is in use. Thus, the history of license datagrams in record 6 provides means for measuring the duration of use of product 1.

Representations of data and records stored at the licensee's site, contained in datagrams, and stored at the licensor's site are illustrated in FIGURE 2. At the licensee's site, network service 7, which handles delivery and transmission of datagrams 3, supplies

network address 8. It is by this address that license control system 4 identifies a location of use of product 1.

Licensed product record 9 is contained within monitor 2. Within the license product record 9 is an identification record 10, which contains the following two items: licensor's network address 11, and product model number 12 that identifies product 1. When a licensor has only one product, or uses different licensor network addresses 11 for each product, product model number 12 may not be needed.

Datagram sent record 13 stores information about the last sent datagram 3. It includes a datagram number 14, which uniquely identifies the last transmitted datagram 3, and the date and time 15 when the last datagram 3 was sent from the licensee's site.

Licensed product record 9 also contains control parameters record 16, which is used for controlling the timing of key events in the communication of license check monitor 2 with license control system 4. Send interval 17 specifies a time interval between each transmission of a new datagram 3 from th licensee to the licensor.

Wait interval 18 is the length of time that monitor 2 waits to receive a reply datagram 3 befor resending the same request datagram 3. The duration of this interval depends on the speed of the communications network being used to deliver datagrams 3.

Disconnect allowed interval 19 is the duration of time that monitor 2 allows product 1 to be used without a reply datagram 3 from the licensor. Th duration of this interval depends on the liability

of the communications network. The interval must be long enough to take into consideration network downtime. For example, suppose a message was sent from the licensor and the network went down just afterwards. Disconnect allowed interval 19 should be long enough to allow the network to resume its normal operation and successfully deliver datagrams 3 from the licensor; otherwise, the licensee would be forced to stop using product 1 until the network was operational.

License datagram 3 contains header 20. Header 20 is used during execution of low level communication protocols within the network. Source network address 21 is the network address from where datagram 3 is sent. Destination network address 22 is the network address to where datagram 3 is sent. Additional data may be included in header 20 if required by low level protocols used in delivering datagrams 3.

Data 23, a part of datagram 3, conveys a message, and contains a number of fields. Product model number 24 and datagram number 25 identify product 1 and datagram 3, respectively. It is noted that retransmitted datagrams have an identical datagram number. Duplicate datagrams must be identified at a licensor's site so that they do not all contribute in billing a licensee.

Each datagram number 25 is unique for each request datagram 3 transmitted from the licensee, except for retransmitted datagrams. This allows a reply datagram 3 received by a licensee to be verified as an actual reply to a request datagram 3 from that licensee, as explained below.

Numb r of proc ss s running 26 is the number of concurrent uses of product 1 at the time datagram 3 is sent. Authorization code 27 is used on reply datagrams 3 to indicate an approval or a denial. Message text 28 contains a message which will be displayed to the user upon a denial.

License database 29 at the licensor's site holds records of information about customers, licenses, and license usage. The types of information within license database 29 of the present embodiment ar shown in FIGURE 2. However, a specific license management system may require its license database to hold types of information other than those in FIGURE 2. For example, licensee name and address may be incorporated as a part of a license database 29.

License record 5 contains information on licenses. Licensee network address 30 identifies a precise network node which is licensed to use product 1. If request datagrams are received which do not originate from known licensee network addresses 30, reply datagrams containing denial messages ar transmitted. Product model number 31 is the mod l number of a licensed product. Termination date 32 is the expiration date of a license. When the license f a product is issued for an unlimited duration, termination date 32 should reflect a date very far into the future, relative to the licensing date.

The present embodiment allows licenses to be paid for in a lease-like or rental fashion. If a licens were to rent or lease product 1, paid through date 33 would reflect the date through which the licensee has paid for using th product. Grac p riod 34 is the time int rval f r which th licens is all w d to be

delinqu nt bef re s rvice ar disc nn ct d. Grac period 34 w uld r flect a v ry large tim interval if the license is not of a lease-like or rental type. When the license provides for a limit on the number of concurrent uses of a product 1, number of processes licensed 35 contains the limiting number. When th license does not provide for such a limit, number of processes 35 should be a very large number.

History of license datagrams 6 is an archive of datagrams 3 received from the licensee.

FIGURE 3 illustrates operations executed at th licensee's site and at the licensor's site. An overview of the processing at the licensee's site is described by steps 101.0 to 106.0, and an overview of the processing at the licensor's site is described by steps 107.0 to 110.0.

At the licensee's site, at step 101.0, product 1 invokes monitor 2. This is accomplished by first establishing monitor 2 as a handler for a timer expiration interrupt signal and for received datagrams 3. Next, a timer is set with a very short time to cause an initial call to monitor 2. At step 102.0, monitor 2 computes a time 36 since the last datagram was sent by determining the difference between the current date and sent time and date and time 15 that a datagram was last sent from the licensee's site. When product 1 commences execution, datagram sent dat and time 15 is set to "null." Thus, time since s nd 36 is very large at the beginning of the monitor's execution. At step 103.0, time since send 36 is compared to send interval 17. If time since send 36 is gr at r than s nd interval 17, th n a r qu st datagram is transmitt d, per th st ps d scribed in

running 26. In th UNIX perating syst m, this procedur could be perform d using th command "ps" t obtain a list of current processes, the command "gr p" to extract the processes of product 1, and "wc" t count the number of processes. Step 103.6 s ts authorization code 27 to number 255 and encrypts th number.

Number 255 indicates that datagram 3 is a request for authorization. Such an indication is needed to guard the present system against the following steps for circumventing the present invention: intercepting outgoing datagrams; and inputting the intercepted datagrams to monitor 2.

Step 103.7 stores the current date and time as sent date & time 15. This date is needed to comput when to send the next datagram 3. Step 103.8 assigns a value to send interval 17, which sets an alarm f r invoking monitor 2 to send the next datagram 3. Step 103.9 sends datagram 3.

In the present embodiment a datagram is transmitted via a connectionless datagram servic . Methods for transmission are well documented for som networking systems. For example, TCP/IP (Transport Control Protocol/Internet Protocol) includes a connectionless protocol called UDP (User Datagram Protocol). A method for sending a datagram using UDP protocol from a SUN Microsystem computer is document d in a SUN manual titled, Network Programming Guide, in section 9 titled "Transport Level Interface Programming."

Step 103.10 sets another alarm using wait int rval 18 for retransmitting datagram 3, if n r ply datagram has be n r c iv d. The alarm caus s monitor

2 to be invok d for ch cking wh ther a reply datagram 3 has be n rec ived. Monit r 2 will transmit a duplicate of the previously transmitted datagram, if no reply has been received. After the execution of step 103.10, "Send License Datagram" procedure returns system control to step 104.0 in FIGURE 3.

FIGURE 5 shows the operation of the "Reply Datagram is Overdue" procedure. Step 104.1 compares time since the last datagram was sent 36 to disconnect allowed interval 19, which, as described above, is th interval that product 1 is allowed to operate even if a reply is overdue. If time since send 36 is smaller than disconnect allowed interval 19, datagram 3 is retransmitted via executing step 103.9 in FIGURE 4. Step 104.2 "disconnects" product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.

Step 104.2 comprises a sequence of sub-steps 104.2.1-104.2.3. Step 104.2.1 assigns number 5 to authorization code 27 in the current datagram being processed. Value 5 is interpreted by monitor 2 as a denial. Step 104.2.2 sets message text 28 to th following: "A reply from licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function." Step 104.2.3 transfers system control to step 105.3 in FIGURE 6. Step 105.3 processes the current denial datagram 3 as if it were just received.

Through the execution of steps 104.1-104.3, th present system permits the use of product 1 for a prescribed period of tim . After the pr scribed

period of time has lapsed, the present system generates a denial.

FIGURE 6 illustrates the steps which monitor 2 follows in processing a reply datagram 3. Step 105.1 decrypts all encrypted data in the received datagram. Step 105.2 compares datagram number 25 with datagram number 14 associated with the last datagram. If datagram number 25 is not equal to datagram number 14, step 105.2 ignores the current datagram and transfers procedural control to step 103.9 (FIGURE 4) in order to resend the last transmitted datagram. After disconnect allowed interval 19 elapses, monitor 2 generates a denial.

In essence, step 105.2 guards against the circumvention of the present invention via: (1) intercepting a reply datagram 3 (from the licensor) containing an approval (2) storing the reply datagram 3; and (3) inputting the stored datagram to monitor 2.

If the execution of step 105.2 does not transfer its procedural control to step 105.3, and if authorization control 27 is not zero (indicating an unqualified authorization has not been received), step 105.3 processes authorization code 27 via steps 105.3.1 to 105.3.3. Step 105.3.1 retrieves message text 28 from datagram 3. If message text 28 is null, then the current datagram 3 is ignored, and monitor 2 resends the last transmitted datagram 3. Step 105.3.1 further protects the present system from attempts to generate fake datagrams and to feed the fake datagrams to monitor 2 by checking for a proper authorization code of zero.

If message text 28 is not null, step 105.3.2 presents the message 28 to the user an output

d vic such as a CRT screen. Step 105.3.3 terminat s the curr nt use of product 1. This st p may be implemented by subroutine or function call to a simpl exit that saves any current user data to a file. Alternatively, product 1 may be designed so that, upon being directed to terminate further execution, it first gives the user an opportunity to save their data.

If authorization code 27 is zero, step 105.4 allows further use of product 1. Step 105.5 returns procedural control to 106.0 on FIGURE 3.

FIGURE 7 shows a sequence of operations within the "Generate Authorization Code" procedure. The procedure produces appropriate authorization code 27 when a request datagram 3 is received at the licensor's site.

Step 108.1 decrypts all encrypted data in the received datagram 3. Using source network address 21 and product model number 24 in the datagram 3, step 108.2 searches the license database 29 for matching licensee network address 30 and product model number 31. If license database 29 does not contain a record of product model number 24 of the product 1 being licensed to the licensee, step 108.3 sets authorization code 27 of its reply datagram 3 to 1 (i.e., the sending node is not a registered address) and authorization is denied.

Step 108.3 prevents copies of product 1 from being installed on multiple nodes independently of whether they are within or outside the licensee's organization. Step 108.3 also prevents the licensee from transporting product 1 from one node to an ther nod with ut th lic nsor's appr val. This is

important because the two nodes may have different processing capacities, and they may be billable at different rates.

If the date a request datagram is received is later than license termination date 32, step 108.4 sets authorization code 27 to number 2 (i.e., license has expired). Step 108.4 allows the licensor to fix licensing periods, or to determine free trial periods for the use of the product. The licensing period may be extended by resetting license termination date 32 at the licensor's site.

If the date when the datagram is received is later than the paid through date 33 as extended by the grace period 34, step 108.5 sets authorization code 27 to 3 (i.e., payment is past due).

If the number of processes running 26 exceeds a licensed number of concurrent uses of product 1 (at a particular node), then step 108.6 sets authorization code 27 to 4 (i.e. concurrent process usage limit is exceeded).

Step 108.7 sets authorization code 27 to 0 indicating processing can continue. It is noted that steps 108.3-108.7 are a part of a

```
IF (x1) then (y1)
ELSE if (x2) then (y2)
ELSE if (x3) then (y3) ...
```

statement of a procedure (e.g., FORTRAN, PASCAL, C, etc). Thus, only one of the steps 108.3-108.7 is executed. Step 108.7 sets authorization code 27 to 0 (indicating approval of further use) only if steps 108.3-108.6 do not execute the THEN portion of each step. Step 108.7 also stores the received datagram 3 in history of license datagrams 6.

Step 108.8 is the last of authorization processing rules 108.1-108.7. After the execution of steps 108.3-108.7, step 108.8 returns procedural control to step 109.0 in FIGURE 3.

FIGURE 8 illustrates the steps which license control system 4 follows to send reply datagram 3 to the licensee.

Step 109.1 encrypts authorization code 27 and writes the encrypted code into datagram 3. Next, step 109.2 writes message text 28 corresponding to authorization code 27 into datagram 3.

Step 109.2 may be replaced with the following method for relaying proper messages to a product user. Proper messages corresponding to each authorization code is stored in monitor 2 at each licensee's site. Upon reception of a reply datagram 3, monitor 2 would locate within itself the proper message corresponding to the authorization code, and use the message for various purposes. This method would reduce the size of reply datagrams 3. However, if the licensor wanted to implement new denial codes, each product would need to somehow incorporate the new message associated with the new denial code into itself. The list of messages, one of which may be written as message text 28, are as follows:

AUTHORIZATION CODE	TEXT MESSAGE
1	This product is not licensed to run at this location. Please contact the licensor to either license this product, or move an existing license of your organization to this location. Use of this product at this

	location is discontinued until this problem is resolved.
2	Your license on this product has expired. Please contact licensor in order to have your licens extended. Use of this product is discontinued until this problem is resolved.
3	Payment on this licensed product is over due and past your grace period. Please have your accounting department send payment in order to continue your license. Use of this product is discontinued until this problem is resolved.
4	Your current use of this licensed product exceeds limits for the number of uses your organization has licensed. Please try again later.
5	A reply from licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function.
0	Authorization is OK. There is no message.

Step 109.3 swaps source network address 21 and destination network address 22. Step 109.4 transmits datagram 3 back to monitor 2.

At step 109.5, a communications network delivers datagram 3 to monitor 2. Subsequently, procedural control returns to step 107.0 in FIGURE 3 to process the next datagram 3.

Although only a few exemplary embodiments of this invention have been described in detail above, those skilled in the art will readily appreciate that many

modifications are possibl in the preferr d embodiments without materially departing fr m th novel teachings and advantages of this invention. For example, product 1 was described as sometimes consisting of information as well as software which controls the information. This approach provides th greatest flexibility, but it is also possible to include the software which controls the information in the networked machine at the licensee's site. In this case, product 1 is split, with part of it on media and part on the licensee's machine. By doing this, some space can be saved on the media containing product 1, but the capabilities of these products will be limited by the standard functions available on these machines.

Also, the presently described embodiment includes a product 1 which is at the licensee's site. This implies that product 1 is on some physical media such as diskette, tape, or CD. However, product 1 can be electronically delivered over communications lines to the licensee and therefore might exist in the memory of the licensee's machine, rather than any physical media. In the case of a product such as music, radio programs and the like, product 1 may even be broadcast to the licensee's site for playback; thus, the product 1 would not even be "resident" in the licensee's machine.

The presently described embodiment allows the licensee to access the licensed product concurrent with the sending and receiving of datagram 3. In this way, the present invention does not inconvenience the legitimate licensee; however, for sensitive licensed products such as c nfid ntial information, th licens

obtaining said facility address that identifies said licensee from said communications facility without any data being provided by said licensee.

51. A method for controlling use of a licensed product comprising the steps of:

generating a request datagram including a facility address that identifies a licensee in a communications facility;

automatically sending said request datagram from a licensee's site over said communications facility to a licensor's site while said licensed product is in use; and

receiving a reply authorizing datagram at said licensee's site and denying the use of said product when no reply authorizing datagram is received.

52. A method as in claim 51 wherein:

said generating step includes the step of incorporating a model number of said product in said datagram.

53. A method as in claim 51, wherein said generating step includes the step of automatically obtaining said facility address that identifies said licensee from said communications facility without any data being provided by said licensee.

54. A method as in claim 51, wherein:

said reply datagram is one of at least a reply authorization datagram and a reply denial datagram; and

said step of automatically sending said request datagram from a licensee's site includes a step of resending said request datagram if neither a reply authorizing datagram nor a reply denial datagram is received within a predetermined time from sending said request datagram from said licensee's site.

55. A method as in claim 51, wherein said step of automatically sending said request datagram from said licensee's site includes the step of sending a request datagram at regular time intervals.

56. A method as in claim 51, wherein:

said generating step includes the step of providing a datagram identification code within said datagram; and

said reply receiving step rejects said reply authorizing datagram if the datagram identification code included in said reply authorizing datagram does not match the datagram identification code included in said request datagram.

57. A method as in claim 51, wherein:

said generating step includes the step of incorporating in said datagram data indicative of the number of processes currently using said product at said licensee's site.

58. A method as in claim 51, further comprising the steps of:

receiving a reply denial datagram; and

displaying, at a licensee's site, a reason for denial when said reply denial datagram is received.

check monitor 2 can prevent access to the product 1 until an authorization reply datagram 3 is received.

Further, monitor 2 could be realized as an integral part of product 1. Monitor 2 could also be implemented as: 1) a separate process which is the parent process of product 1 (Such a parent process would have the authority to cancel the use of product 1); 2) a single system level task which controls license checking of all products at the licens 's site; and 3) custom logic in a digital integrated circuit (the present invention could be implement d as hardware instead of software).

Also, though the above embodiment has been described as being implemented on a computer system network where operator messages are provided on a CRT monitor or the like, the invention may be practiced on other hardware platforms by incorporating appropriate changes known to those of ordinary skill in the art. For example, in an alternative hardware embodiment such as a music or video playback devic , monitor 2 is invoked by the licensee's action of pushing the "play" or similar button, and in a broadcast music application or similar system, th monitor may be invoked simply by turning the devic on. The processing of monitor 2 is as described in the presently described embodiment. However, wh n a denial message is received or generated, monitor 2 must be able to switch "play" to "off".

The presently described embodiment is design d to be used in conjunction with a connectionless UDP (User Datagram Protocol) in the TCP/IP protocol suit as an underlying pr tocol. Howev r, the pr s nt invention could also be r aliz d using a slow r,

connectionless protocol such as electronic mail or a variety of connection protocols (e.g., File Transfer Protocols (FTP), Telnet).

It is noted that protocol suites quite different from TCP/IP could be used, such as ISO (International Standards Organization) protocol. In addition, datagrams 3 could be sent over telephone systems with communications protocols such as those specified by CCITT (Consultative Committee on International Telephony and Telegraphy). In this case, telephone numbers could serve as network addresses 21, 22. Communications protocols for wireless communications such as cellular telephone can also be used to send the datagram 3.

Accordingly, all such modifications are intended to be included within the scope of this invention as defined by the following claims.

WHAT IS CLAIMED IS:

1. A method for monitoring the use of a licensed product, comprising the steps of:

generating, at regular time intervals, datagrams including an address in a communications facility, said facility address identifying a licensee;

automatically sending said datagrams from at least one licensee's site over said facility to a licensor's site while said licensed product is in use;

receiving said datagrams at said licensor's site;

storing an indication of receipt of each f said datagrams; and

counting said datagrams from each licens e as an indication of the use by the licensee of said licensed product.

2. A method as in claim 1 further wherein:

said generating step includes the step of incorporating a model number of said product in said datagrams; and

said counting step includes the step of separately counting datagrams for each product mod l number for each licensee.

3. A method as in claim 1, wherein said generating step includes the step of automatically obtaining said facility address that identifies said licensee from said facility without any data being provid d by said lic nsee.

4. A method for controlling use of a licensed product comprising the steps of:

generating a request datagram including an address in a communications facility, said facility address identifying a licensee;

automatically sending said request datagram from at least one licensee's site over said facility to a licensor's site while said licensed product is in use;

receiving said request datagram at said licensor's site;

comparing said received request datagram with rules and license data at said licensor's site to determine if use of said licensed product is authorized;

sending a reply authorizing datagram to said licensee's site if use of said licensed product is approved; and

receiving said reply authorizing datagram at said licensee's site and denying the use of said product when no reply authorizing datagram is received.

5. A method as in claim 4, wherein:

said generating step includes the step of incorporating a model number of said product in said datagram;

said comparing step includes the step of comparing said rules and license data for a particular model number; and

said sending step includes the step of transmitting said reply datagram for each product model number.

6. A method as in claim 4, wherein said generating step includes the step of automatically obtaining said facility address that identifies said licensee from said facility without any data being provided by said licensee.

7. A method as in claim 4 further comprising the step of sending a reply denial datagram if use of said licensed product is not approved as determined in said comparing step, said step of automatically sending said request datagram from a licensee's site including the step of resending said request datagram if neither a reply authorizing datagram nor a reply denial datagram is received from said licensor's site within a predetermined time from sending said request datagram from said licensee's site.

8. A method as in claim 4, wherein said step of automatically sending said request datagram from said licensee's site includes the step of sending a request datagram at regular time intervals.

9. A method as in claim 4, wherein:

said generating step includes the step of providing a datagram identification code within said datagram;

said reply datagram sending step includes the step of inserting the same datagram identification code in said reply datagram; and

said reply receiving step rejects said reply authorizing datagram if the datagram identification code included in said reply authorizing datagram does

not match the datagram identification code included in said request datagram.

10. A method as in claim 4, wherein:

said comparing step includes the step of comparing said facility address that identifies said licensee with a list of valid licensee addresses to determine if said facility address is a valid address; and

said reply authorizing datagram is not sent if said facility address that identifies said licensee is not valid.

11. A method as in claim 10 further comprising the step of sending a reply denial datagram if said facility address that identifies said licensee is not valid.

12. A method as in claim 4, wherein:

said comparing step includes the step of comparing a license expiration date with a date at which said datagram is received; and

said reply authorizing datagram is not sent if the license expiration date is later than the date at which said datagram is received.

13. A method as in claim 12, further comprising the step of sending a reply denial datagram if the license expiration date is later than the date at which said datagram is received.

14. A m thod as in claim 4, wher in:

said comparing step includes the step of checking currentness of payments from said licensee; and

said reply authorizing datagram is not sent if payment is overdue.

15. A method as in claim 14, further comprising the step of sending a reply denial datagram if payment is overdue.

16. A method as in claim 4, wherein:

said generating step includes the step of incorporating in said datagram data indicative of th number of processes currently using said product at said licensee's site;

said comparing step includes the step of comparing the number of processes using said product at the licensee's site to an authorized number; and

said reply authorizing datagram is not sent if said number of processes using said product exceeds said authorized number.

17. A method as in claim 16, further comprising the step of sending a reply denial datagram if said number of processes using said product exceeds said authorized number.

18. A method as in claim 4, wherein said sending step includes the steps of sending said reply authorizing datagram when use of said product is approved and sending a reply denial datagram when us f said product is n t approved, said r c iving st p

d nying use of said product when said r ply d nial datagram is receiv d.

19. A method as in claim 18, wherein said receiving and denying step denies use of said product when neither a reply authorizing datagram nor a reply denial datagram is received within a predetermined time after said request datagram is sent.

20. A method as in claim 18, further comprising the step of indicating, at a licensee's site, a reas n for denial when said reply denial datagram is received.

21. A method as in claim 4, wherein:

said licensed product comprises an executable portion and a data portion; and

said method further comprises a step f controlling use of said data portion with said executable portion.

22. A method as in claim 4 further comprising a step of allowing use of said licensed product befor a reply datagram is received.

23. A system for controlling licensed product comprising:

a communications facility to which at least one licensee having a license for operating a licens d product from the licensor is connected;

monitoring means, connected to said facility at a sit of each said licens e, for generating a r qu st datagram including an addr ss of said licens

on said facility and transmitting said request datagram over said facility t a sit f said licensor, and for receiving and processing a reply datagram; and

controlling means, connected to said facility at said licensor's site, for receiving said request datagram, comparing said request datagram with rules and license data to determine if use of said licensed product is authorized and sending a reply authorizing datagram to said licensee's site if use of said product is approved; and

said monitoring means including means for denying use of said licensed product when no reply authorizing datagram is received.

24. A system as in claim 23, wherein:

said monitoring means sends requ st datagrams at regular time intervals during use of said licensed product; and

said controlling means further compris s means for counting said request datagrams received at said controlling means and means for computing an amount to be billed to said licensee in response to said counting.

25. A system as in claim 23 wherein:

said monitoring means incorporates a model number for said product in said request datagram; and

said controlling means comprises means f r counting datagrams for each product model number f r each licensee, in order to compute an amount to be billed t ach licens .

26. A system as in claim 23, wh rein said monitoring means automatically obtains said facility address of said licensee from said facility without any input from said licensee.

27. A system as in claim 23, wherein:

said controlling means sends a reply denial datagram to said licensee's site if use of said product is not approved; and

said monitoring means resends said request datagram if no reply authorizing datagram and no reply denial datagram is received within a predetermined period of time after said requesting datagram is sent.

28. A system as in claim 23, wherein said monitoring means transmits request datagrams at predetermined time intervals.

29. A system as in claim 23, wherein:

said monitoring means incorporates a unique identification code in said request datagram;

said controlling means incorporates the sam request datagram identification code in said reply authorizing datagram; and

said monitoring means rejects any reply authorizing datagram which does not include the sam identification code as included in said request datagram.

30. A system as in claim 23, wherein said controlling means compares said facility address of said lic nsee with a list f valid lic nse facility addr ss s and do s n t gen rat a r ply authorizing

datagram if said facility address of said licens is not valid.

31. A system as in claim 30, wherein said controlling means sends a reply denial datagram wh n said facility address is not valid.

32. A system as in claim 23, wherein said controlling means compares an expiration date of a license of said product with a date at which said request datagram is received by said controlling means, and does not generate a reply authorizing datagram, thus denying use of said product, if th license expiration date is earlier than the date at which said request datagram is received.

33. A system as in claim 32, wherein said controlling means sends a reply denial datagram if th license expiration date is earlier than the date at which said request datagram is received.

34. A system as in claim 23, wherein said controlling means generates a reply authorizing datagram, thus denying use of said product, if a payment for the use of said product is overdue.

35. A system as in claim 34, wherein said controlling means sends a reply denial datagram if payment for the use of said product is overdue.

36. A system as in claim 23, wherein:

said monit ring m ans includ s in said request datagram data indicative f the number of

proc ss s, at a licens e's sit , currently using said product; and

said controlling means does not generate a reply authorizing datagram, thus denying a use of said product, if more than a predetermined number of processes using said product are running at the licensee's site.

37. A system as in claim 36, wherein said controlling means sends a reply denial datagram if more than said predetermined number of processes using said product are running at the licensee's site.

38. A system as in claim 23, wherein said controlling means sends a reply denial datagram if use of said product is not approved.

39. A system as in claim 38, wherein said monitoring means denies use of said licensed product when no reply authorizing datagram and no reply denial datagram is received within a predetermined time from the sending of said request datagram.

40. A system as in claim 38, further comprising means for indicating, at a licensee's site, a reas n for denial when said reply denial datagram is received.

41. A system as in claim 23, wherein:

said licensed product comprises an executabl portion and a data portion; and

said system further comprises means for controlling use of said data portion with said executable portion.

42. A system as in claim 41, wherein said data portion controlling means is disposed within said executable portion.

43. A system as in claim 41, wherein said data portion controlling means comprises a first partial controlling means disposed within said executabl portion and a second partial controlling means disposed within said monitoring means.

44. A system as in claim 23, wherein said monitoring means includes means for permitting use of said licensed product before a reply datagram is received.

45. A system for monitoring product comprising:

a communications facility to which at least one licensee having a license for operating a licensed product from a licensor is connected;

monitoring means, connected to said facility at a site of each said licensee, for generating datagrams including an address of said licensee n said facility and transmitting said datagrams at periodic intervals over said facility to a site f said licensor; and

control means, connected to said facility at said licensor's site, for receiving said requ st datagrams, st ring an indication f receipt of ach f said datagrams and counting said datagrams from ach

lic ns as an indication of th us by the lic nse of said licensed product.

46. A system as in claim 45, wherein said monitoring means automatically obtains said facility address of said licensee from said facility without any input from said licensee.

47. A system as in claim 45, wherein:

said monitoring means incorporates a product model number in said request datagrams; and

said controlling means separately counts request datagrams for each product model number for each licensee.

48. A method for monitoring the use of a licensed product comprising the steps of:

generating, at regular time intervals, datagrams including an address in a communications facility, said facility address identifying a licensee; and

automatically sending said datagrams from at least one licensee's site over said communications facility to a licensor's site while said licensed product is in use.

49. A method as in claim 48 further wherein:

said generating step includes the step of incorporating a model number of said product in said datagrams.

50. A m thod as in claim 48, wher in said g n rating step includ s th st p of automatically

btaining said facility address that id ntifi s said licensee fr m said communications facility without any data being provided by said licensee.

51. A method for controlling use of a licens d product comprising the steps of:

generating a request datagram including a facility address that identifies a licensee in a communications facility;

automatically sending said request datagram from a licensee's site over said communications facility to a licensor's site while said licens d product is in use; and

receiving a reply authorizing datagram at said licensee's site and denying the use of said product when no reply authorizing datagram is received.

52. A method as in claim 51 wherein:

said generating step includes the step of incorporating a model number of said product in said datagram.

53. A method as in claim 51, wherein said generating step includes the step of automatically obtaining said facility address that identifies said licensee from said communications facility without any data being provided by said licensee.

54. A method as in claim 51, wherein:

said reply datagram is one of at least a reply authorizati n datagram and a reply denial datagram; and

said step of automatically sending said request datagram from a licensee's site includes a step of resending said request datagram if neither a reply authorizing datagram nor a reply denial datagram is received within a predetermined time from sending said request datagram from said licensee's site.

55. A method as in claim 51, wherein said step of automatically sending said request datagram from said licensee's site includes the step of sending a request datagram at regular time intervals.

56. A method as in claim 51, wherein:

said generating step includes the step of providing a datagram identification code within said datagram; and

said reply receiving step rejects said reply authorizing datagram if the datagram identification code included in said reply authorizing datagram does not match the datagram identification code included in said request datagram.

57. A method as in claim 51, wherein:

said generating step includes the step of incorporating in said datagram data indicative of the number of processes currently using said product at said licensee's site.

58. A method as in claim 51, further comprising the steps of:

receiving a reply denial datagram; and

displaying, at a license's site, a reason for denial when said reply denial datagram is received.

59. A method as in claim 51, wherein:

said licensed product comprises an executabl portion and a data portion; and

said method further comprises a step f controlling use of said data portion with said executable portion.

60. A method as in claim 51 further comprising a step of allowing use of said licensed product before a reply datagram is received.

61. A system for controlling a licensed product comprising:

a communications facility to which at least one licensee is connected;

monitoring means, connected to said communications facility at a site of each said licensee, for generating a request datagram including an address of said licensee on said communications facility and transmitting said request datagram ov r said communications facility, and for receiving and processing a reply authorizing datagram; and

means for denying use of said product when n reply authorizing datagram is received.

62. A system as in claim 61, wherein:

said monitoring means sends request datagrams at regular time intervals during use of said licensed product.

63. A system as in claim 61 wh r in:

said monitoring means incorporates a model number for said product in said request datagram.

64. A system as in claim 61, wherein said monitoring means automatically obtains said facility address of said licensee from said communications facility without any input from said licensee.

65. A system as in claim 61, wherein:

said monitoring means resends said request datagram if no reply authorizing datagram and no reply denial datagram is received within a predetermined period of time after said requesting datagram is sent.

66. A system as in claim 61, wherein said monitoring means transmits request datagrams at predetermined time intervals.

67. A system as in claim 61, wherein:

said monitoring means incorporates a unique identification code in said request datagram; and

said monitoring means rejects any reply authorizing datagram which does not include the same identification code as included in said request datagram.

68. A system as in claim 61, wherein:

said monitoring means includes in said request datagram data indicative of the number of processes, at a licensee's site, currently using said product.

69. A system as in claim 61, wherein:

said monitoring means denies use of said licensed product when no reply authorizing datagram and no reply denial datagram is received within a predetermined time from the sending of said request datagram.

70. A system as in claim 61, further comprising means for indicating, at a licensee's site, a reason for denial when a reply denial datagram is received.

71. A system as in claim 61, wherein:

said licensed product comprises an executable portion and a data portion; and

said system further comprises means for controlling use of said data portion with said executable portion.

72. A system as in claim 71, wherein said data portion controlling means is disposed within said executable portion.

73. A system as in claim 71, wherein said data portion controlling means comprises a first partial controlling means disposed within said executable portion and a second partial controlling means disposed within said monitoring means.

74. A system as in claim 61, wherein said monitoring means includes means for permitting use of said licensed product before a reply datagram is received.

75. A system for monitoring a lic nsed product comprising:

a communications facility to which at least one licensee is connected;

monitoring means, connected to said communications facility at a site of each said licensee, for generating datagrams including an address of said licensee on said communications facility and transmitting said datagrams at periodic intervals over said communications facility.

76. A system as in claim 75, wherein said monitoring means automatically obtains said communications facility address of said licensee from said communications facility without any input from said licensee.

77. A system as in claim 75, wherein:

said monitoring means incorporates a product model number in said request datagrams.

78. A method for monitoring the use of a licensed product comprising the steps of:

receiving datagrams at a licensor's site on a communications facility having at least one licensee's site thereon, said datagrams being generated at regular time intervals and including a facility address that identifies a licensee in said communications facility;

storing an indication of receipt of each of said datagrams; and

counting s id datagrams as an indication of th us of said lic nsed product.

75. A system for monitoring a licensed product comprising:

a communications facility to which at least one licensee is connected;

monitoring means, connected to said communications facility at a site of each said licensee, for generating datagrams including an address of said licensee on said communications facility and transmitting said datagrams at periodic intervals over said communications facility.

76. A system as in claim 75, wherein said monitoring means automatically obtains said communications facility address of said licensee from said communications facility without any input from said licensee.

77. A system as in claim 75, wherein:

said monitoring means incorporates a product model number in said request datagrams.

78. A method for monitoring the use of a licensed product comprising the steps of:

receiving datagrams at a licensor's site on a communications facility having at least on licensee's site thereon, said datagrams being generated at regular time intervals and including a facility address that identifies a licensee in said communications facility;

storing an indication of receipt of each of said datagrams; and

counting said datagrams as an indicati n f th us of said lic nsed product.

79. A method as in claim 78 further wherein:

said datagrams include a model number of each product; and

said counting step includes the step of separately counting datagrams for each product model number for each licensee.

80. A method for controlling use of a licensed product comprising the steps of:

receiving a request datagram at a licensor's site on a communications facility having at least one licensee's site thereon, said request datagram including a facility address identifying a license and being automatically sent over said communications facility to said licensor's site while said licensed product is in use;

comparing said received request datagram with rules and license data at said licensor's site to determine if use of said licensed product is authorized; and

sending a reply authorizing datagram if use of said licensed product is approved.

81. A method as in claim 80 wherein:

said datagrams include a model number of said product;

said comparing step includes the step of comparing said rules and license data for a particular model number; and

said sending step includes the step of transmitting said reply datagram for each product model number.

82. A method as in claim 80 further comprising the step of sending a reply denial datagram if use of said licensed product is not approved as determined in said comparing step.

83. A method as in claim 80, wherein:

said datagrams include a datagram identification code; and

said reply datagram sending step includes the step of inserting the same datagram identification code in said reply datagram.

84. A method as in claim 80, wherein:

said comparing step includes the step of comparing said facility address that identifies said licensee with a list of valid licensee addresses to determine if said facility address is a valid address; and

said reply authorizing datagram is not sent if said facility address that identifies said licensee is not valid.

85. A method as in claim 84 further comprising the step of sending a reply denial datagram if said facility address that identifies said licensee is not valid.

86. A method as in claim 80, wherein:

said comparing step includes the step of comparing a license expiration date with a date at which said datagram is r ceiv d; and

said reply authorizing datagram is not sent if the license expiration date is later than the dat at which said datagram is received.

87. A method as in claim 86, further comprising the step of sending a reply denial datagram if th license expiration date is later than the date at which said datagram is received.

88. A method as in claim 80, wherein:

said comparing step includes the step of checking currentness of payments from said licens ; and

said reply authorizing datagram is not sent if payment is overdue.

89. A method as in claim 88, further comprising the step of sending a reply denial datagram if paym nt is overdue.

90. A method as in claim 80, wherein:

said datagrams include data indicative of the number of processes currently using said product at said licensee's site;

said comparing step includes the step of comparing a number of processes using said product t an authorized number; and

said reply authorizing datagram is not sent if said number of processes using said product exce ds said authoriz d number.

91. A method as in claim 90, furth r comprising th st p of s nding a reply denial datagram if said

number of processes using said product exceeds said authorized number.

92. A method as in claim 80, wherein said sending step includes the steps of sending said reply authorizing datagram when use of said product is approved and sending a reply denial datagram when use of said product is not approved.

93. A system for controlling a licensed product comprising:

a communications facility to which at least one licensee and a licensor are connected at a licensee's site and at a licensor's site, respectively; and

controlling means, connected to said communications facility at said licensor's site, for: receiving a request datagram, said request datagram including an address of said licensee on said communications facility and being transmitted over said communications facility to a site of said licensor; comparing said request datagram with rules and license data to determine if use of said licensed product is authorized; and sending a reply authorizing datagram to said licensee's site if use of said product is approved.

94. A system as in claim 93, wherein:

said request datagrams are sent at regular time intervals during use of said licensed product; and

said controlling means comprises means for counting said request datagrams received at said

99. A system as in claim 98, wherein said controlling means sends a reply denial datagram when said facility address is not valid.

100. A system as in claim 93, wherein said controlling means compares an expiration date of a license of said product with a date at which said request datagram is received by said controlling means, and does not generate a reply authorizing datagram, thus denying use of said product, if the license expiration date is earlier than the date at which said request datagram is received.

101. A system as in claim 100, wherein said controlling means sends a reply denial datagram if th license expiration date is earlier than the date at which said request datagram is received.

102. A system as in claim 93, wherein said controlling means generate a reply authorizing datagram, thus denying use of said product, if a payment for the use of said product is overdue.

103. A system as in claim 102, wherein said controlling means sends a reply denial datagram if payment for the use of said product is overdue.

104. A system as in claim 93, wherein:

said datagrams include data indicative f the number of processes, at a licensee's sit , currently using said product; and

said c ntrolling m ans d s not g n rate a r ply authorizing datagram, thus denying a us of said

product, if more than a predetermined number of processes using said product are running at the licensee's site.

105. A system as in claim 104, wherein said controlling means sends a reply denial datagram if more than said predetermined number of processes using said product are running at the licensee's site.

106. A system as in claim 93, wherein said controlling means sends a reply denial datagram if use of said product is not approved.

107. A system as in claim 93, wherein:

said licensed product comprises an executable portion and a data portion; and

said system further comprises means for controlling use of said data portion with said executable portion.

108. A system as in claim 107, wherein said data portion controlling means is disposed within said executable portion.

109. A system for monitoring a licensed product comprising:

a communications facility to which at least one licensee and a licensor are connected at a licensee's site and at a licensor's site, respectively; and

control means, connected to said communications facility at a licensor's site, for: receiving request datagrams, said request datagrams

including an address of said licensee in said communications facility and being transmitted at periodic intervals over said communications facility to said licensor's site; storing an indication of receipt of each of said datagrams; and counting said datagrams from each licensee as an indication of the use by the licensee of said licensed product.

110. A system as in claim 110, wherein:

said request datagrams include a product model number; and

said controlling means separately counts request datagrams for each product model number for each licensee.

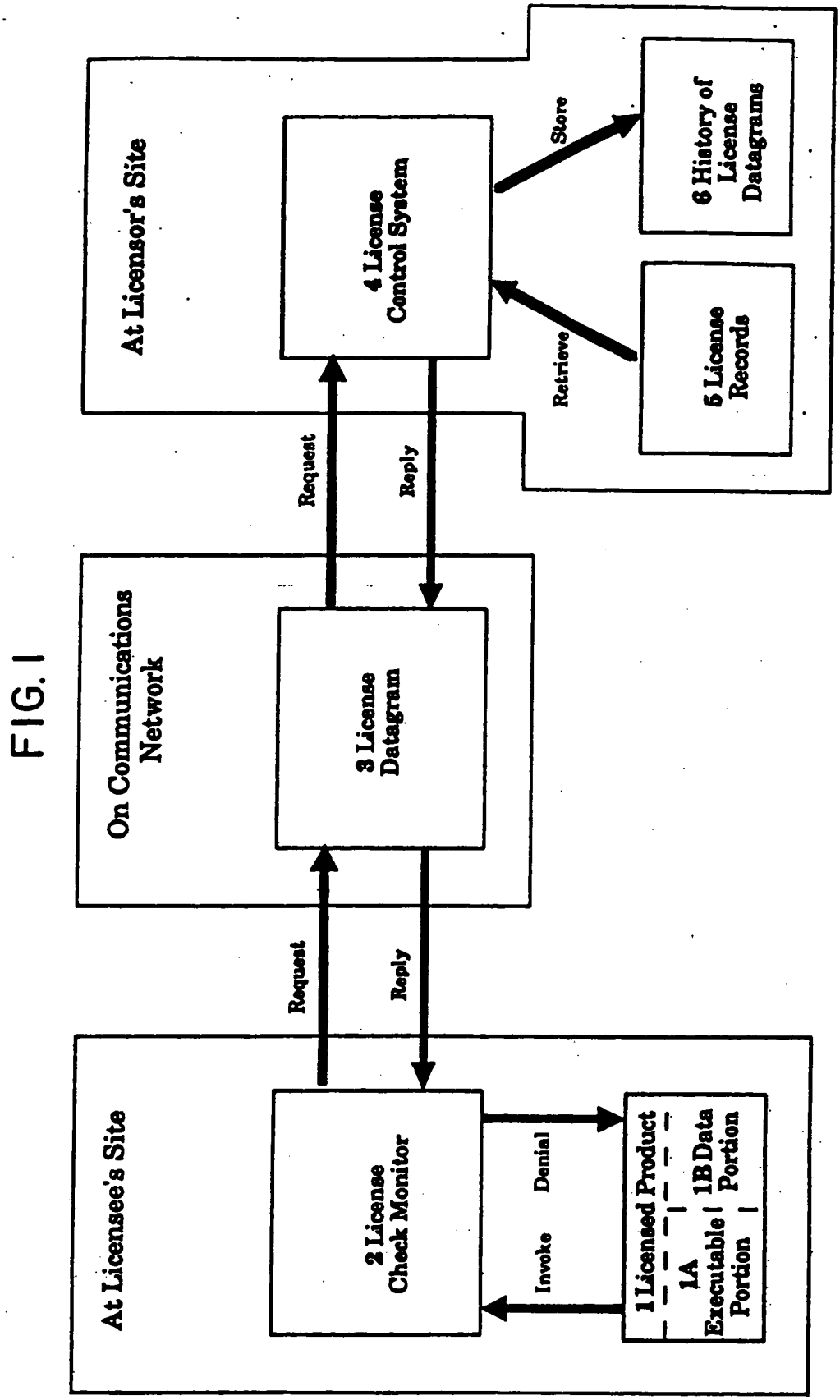

At Licensor's Site
4 License Control System
Store
6 History of License Datagrams
Retrieve
5 License Records
Request
Reply
On Communications Network
3 License Datagram
Request
Reply
At Licensee's Site
2 License Check Monitor
Denial
Invoke
1 Licensed Product
1A Executable Portion
1B Data Portion

FIG. 1

FIG. 2

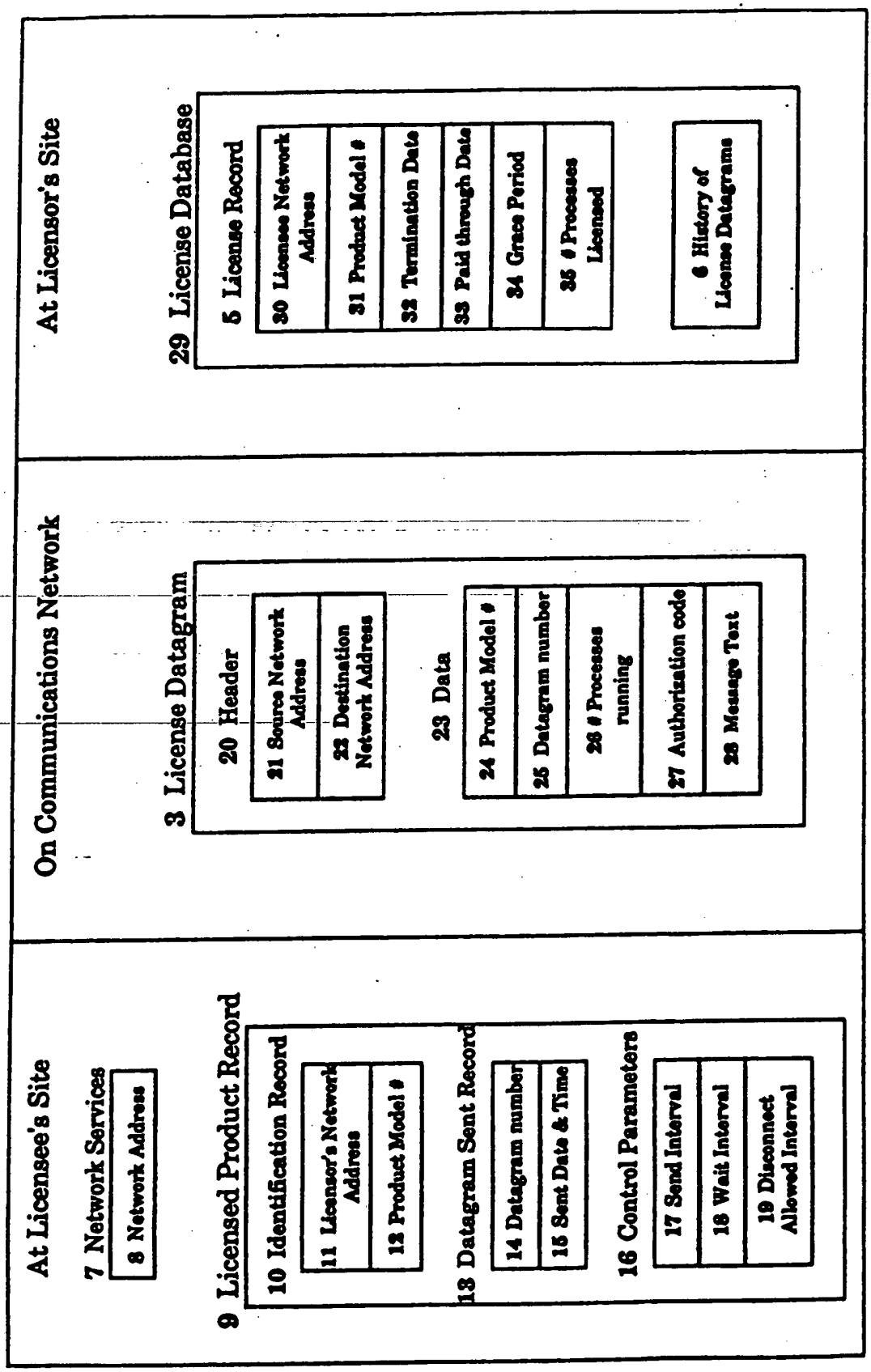

At Licensee's Site
7 Network Services
8 Network Address
9 Licensed Product Record
10 Identification Record
11 Licensor's Network Address
12 Product Model #
13 Datagram Sent Record
14 Datagram number
15 Sent Date & Time
16 Control Parameters
17 Send Interval
18 Wait Interval
19 Disconnect Allowed Interval
On Communications Network
3 License Datagram
20 Header
21 Source Network Address
22 Destination Network Address
23 Data
24 Product Model #
25 Datagram number
26 # Processes running
27 Authorisation code
28 Message Text
At Licensor's Site
29 License Database
5 License Record
30 Licensee Network Address
31 Product Model #
32 Termination Date
33 Paid through Date
34 Grace Period
35 # Processes Licensed
6 History of License Datagrams

FIG. 3

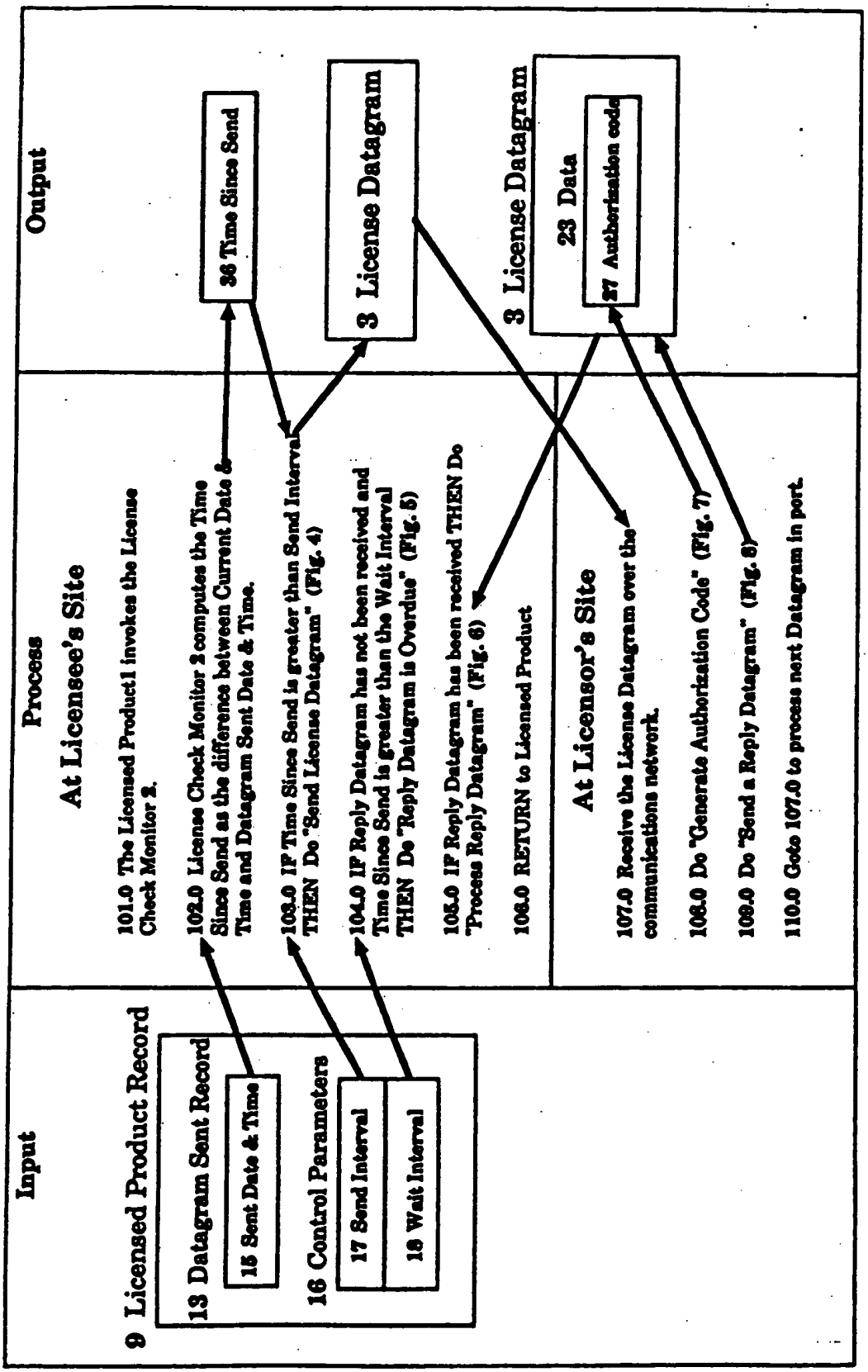

Input
9 Licensed Product Record
13 Datagram Sent Record
15 Sent Date & Time
16 Control Parameters
17 Send Interval
18 Wait Interval
Process
At Licensee's Site
101.0 The Licensed Product1 invokes the License Check Monitor 2.
102.0 License Check Monitor 2 computes the Time Since Send as the difference between Current Date & Time and Datagram Sent Date & Time.
103.0 IF Time Since Send is greater than Send Interval THEN Do "Send License Datagram" (Fig. 4)
104.0 IF Reply Datagram has not been received and Time Since Send is greater than the Wait Interval THEN Do "Reply Datagram is Overdue" (Fig. 5)
105.0 IF Reply Datagram has been received THEN Do "Process Reply Datagram" (Fig. 6)
106.0 RETURN to Licensed Product
At Licensor's Site
107.0 Receive the License Datagram over the communications network.
108.0 Do "Generate Authorization Code" (Fig. 7)
109.0 Do "Send a Reply Datagram" (Fig. 8)
110.0 Goto 107.0 to process next Datagram in port.
Output
26 Time Since Send
3 License Datagram
3 License Datagram
23 Data
27 Authorization code

FIG. 4

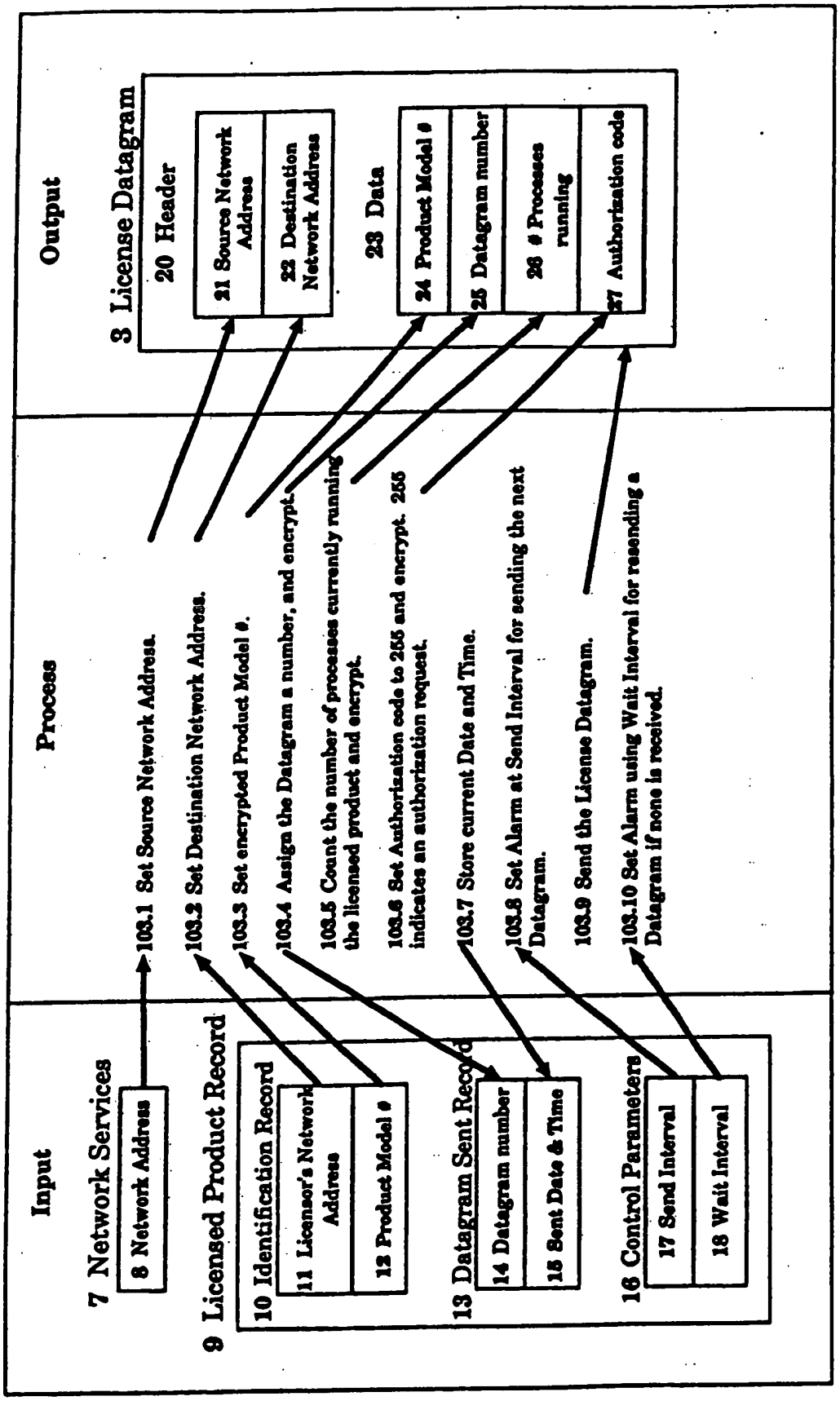

Input
Process
Output
7 Network Services
8 Network Address
9 Licensed Product Record
10 Identification Record
11 Licensor's Network Address
12 Product Model #
13 Datagram Sent Record
14 Datagram number
15 Sent Date & Time
16 Control Parameters
17 Send Interval
18 Wait Interval
3 License Datagram
20 Header
21 Source Network Address
22 Destination Network Address
23 Data
24 Product Model #
25 Datagram number
26 # Processes running
27 Authorization code
103.1 Set Source Network Address.
103.2 Set Destination Network Address.
103.3 Set encrypted Product Model #.
103.4 Assign the Datagram a number, and encrypt.
103.5 Count the number of processes currently running the licensed product and encrypt.
103.6 Set Authorization code to 255 and encrypt. 255 indicates an authorization request.
103.7 Store current Date and Time.
103.8 Set Alarm at Send Interval for sending the next Datagram.
103.9 Send the License Datagram.
103.10 Set Alarm using Wait Interval for resending a Datagram if none is received.

FIG. 5

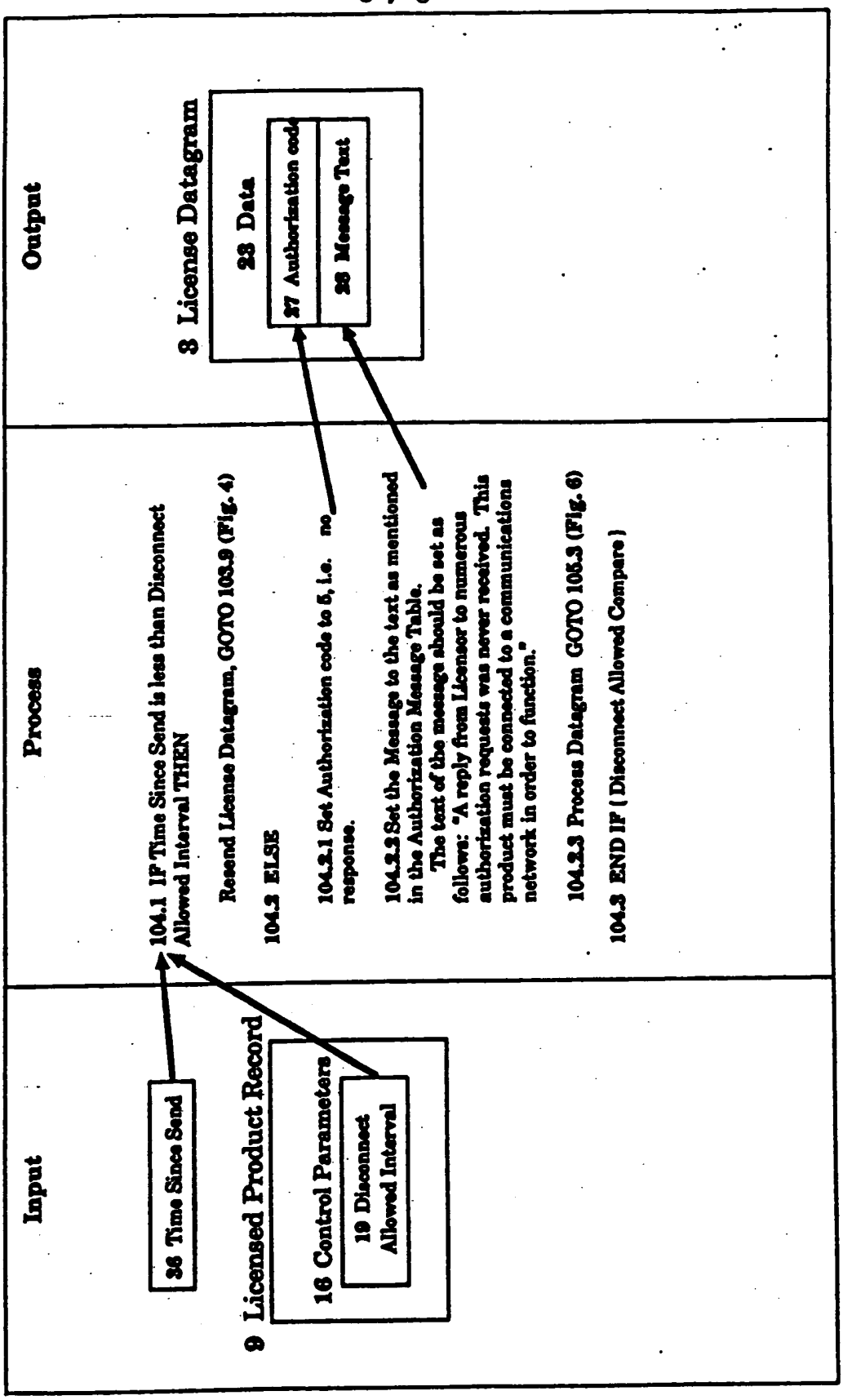

Input
Process
Output
26 Time Since Send
9 Licensed Product Record
16 Control Parameters
19 Disconnect Allowed Interval
104.1 IF Time Since Send is less than Disconnect Allowed Interval THEN
Resend License Datagram, GOTO 105.9 (Fig. 4)
104.2 ELSE
104.2.1 Set Authorization code to 5, i.e. no response.
104.2.2 Set the Message to the text as mentioned in the Authorization Message Table.
The text of the message should be set as follows: "A reply from Licenser to numerous authorization requests was never received. This product must be connected to a communications network in order to function."
104.2.3 Process Datagram GOTO 105.3 (Fig. 6)
104.3 END IF (Disconnect Allowed Compare)
3 License Datagram
23 Data
27 Authorization code
28 Message Text

FIG. 6

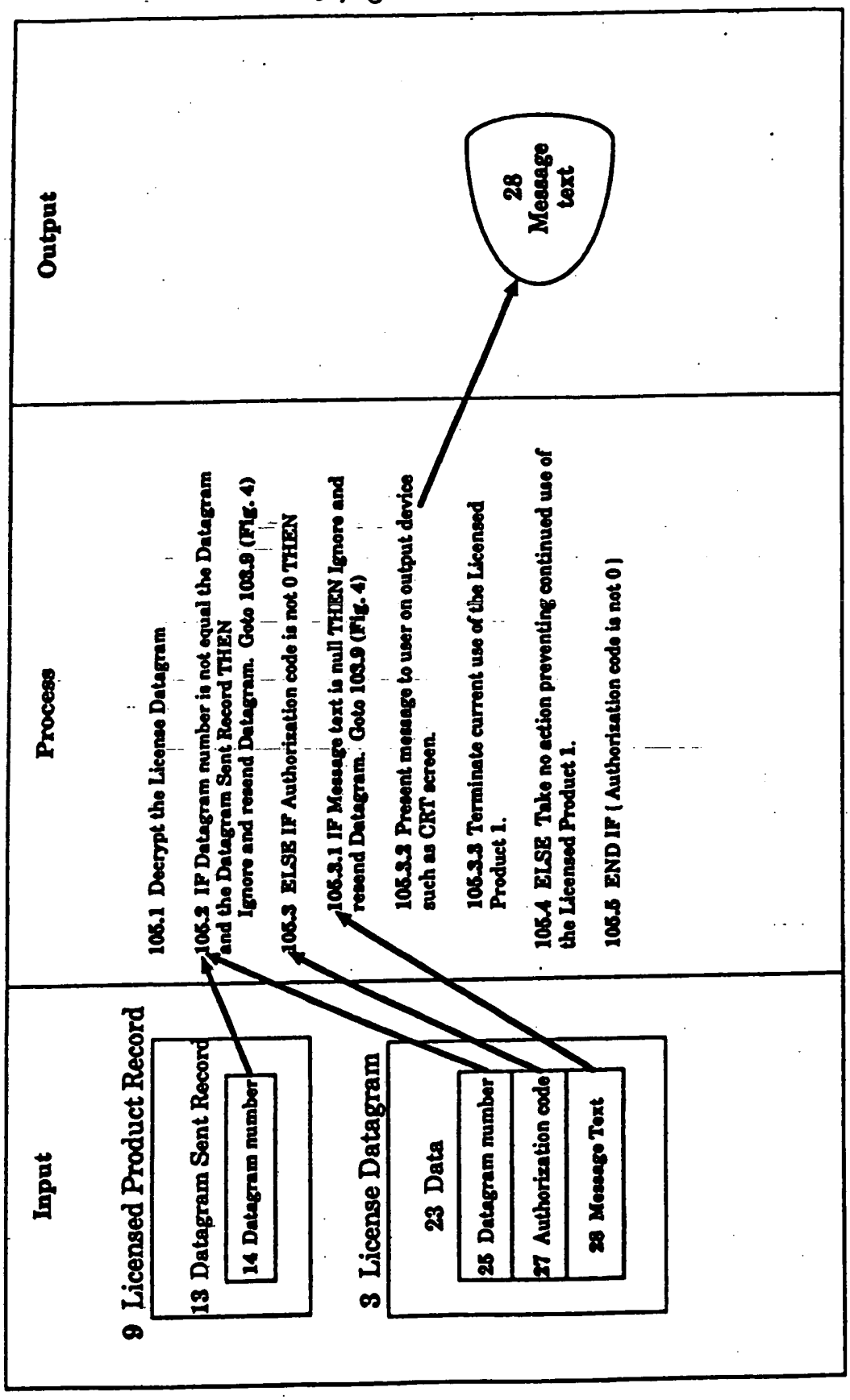
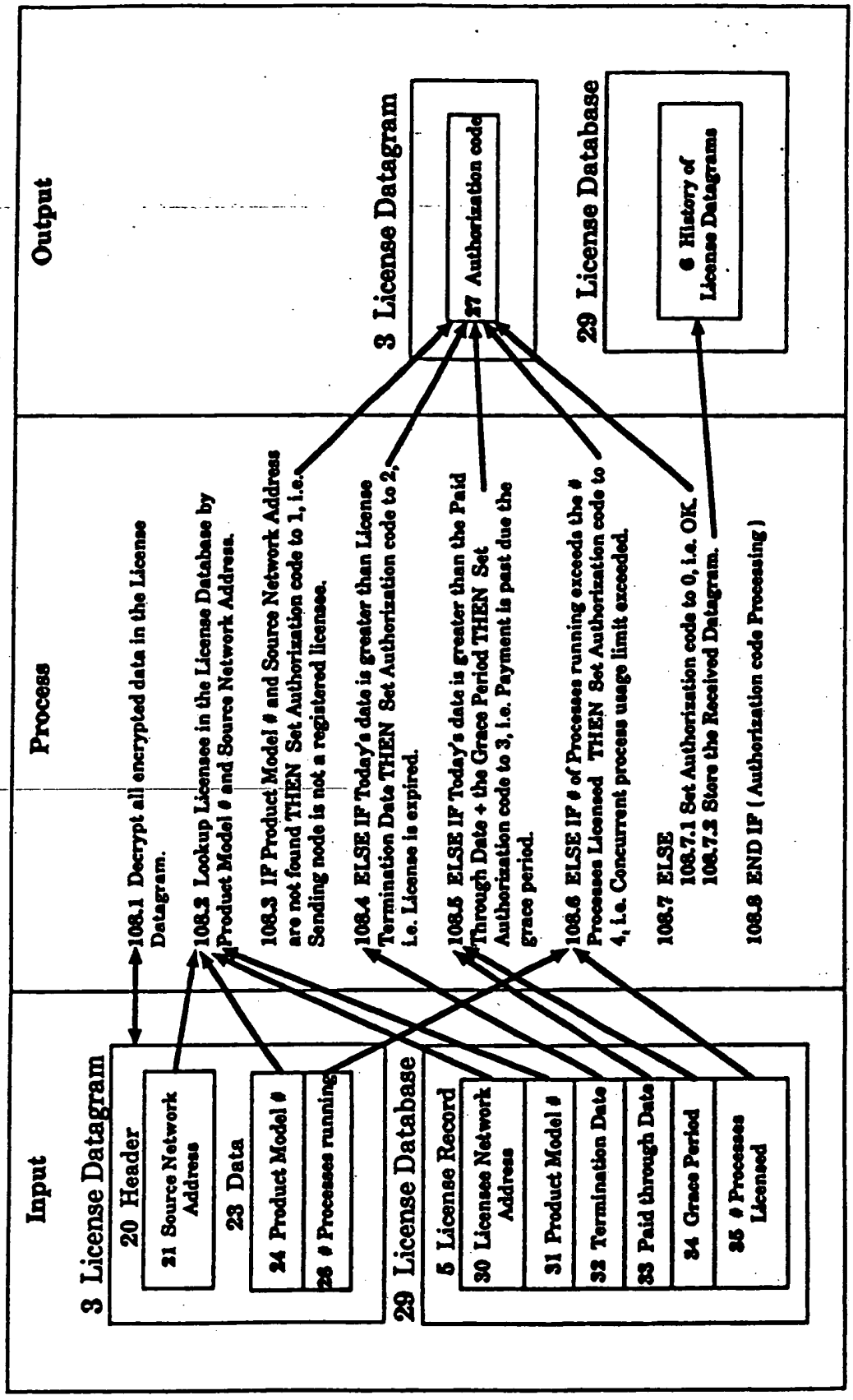

Input
Process
Output
9 Licensed Product Record
13 Datagram Sent Record
14 Datagram number
3 License Datagram
23 Data
25 Datagram number
27 Authorization code
28 Message Text
105.1 Decrypt the License Datagram
105.2 IF Datagram number is not equal the Datagram and the Datagram Sent Record THEN Ignore and resend Datagram. Goto 103.9 (Fig. 4)
105.3 ELSE IF Authorization code is not 0 THEN
105.3.1 IF Message text is null THEN Ignore and resend Datagram. Goto 103.9 (Fig. 4)
105.3.2 Present message to user on output device such as CRT screen.
105.3.3 Terminate current use of the Licensed Product 1.
105.4 ELSE Take no action preventing continued use of the Licensed Product 1.
105.5 END IF (Authorization code is not 0)
28 Message text

FIG. 7


Output
Process
Input
3 License Datagram
20 Header
21 Source Network Address
23 Data
24 Product Model #
26 # Processes running
29 License Database
5 License Record
30 Licensee Network Address
31 Product Model #
32 Termination Date
33 Paid through Date
34 Grace Period
35 # Processes Licensed
3 License Datagram
37 Authorization code
29 License Database
6 History of License Datagrams
108.1 Decrypt all encrypted data in the License Datagram.
108.2 Lookup Licensee in the License Database by Product Model # and Source Network Address.
108.3 IF Product Model # and Source Network Address are not found THEN Set Authorization code to 1, i.e. Sending node is not a registered licensee.
108.4 ELSE IF Today's date is greater than License Termination Date THEN Set Authorization code to 2, i.e. License is expired.
108.5 ELSE IF Today's date is greater than the Paid Through Date + the Grace Period THEN Set Authorization code to 3, i.e. Payment is past due the grace period.
108.6 ELSE IF # of Processes running exceeds the # Processes Licensed THEN Set Authorization code to 4, i.e. Concurrent process usage limit exceeded.
108.7 ELSE
108.7.1 Set Authorization code to 0, i.e. OK.
108.7.2 Store the Received Datagram.
108.8 END IF (Authorization code Processing)

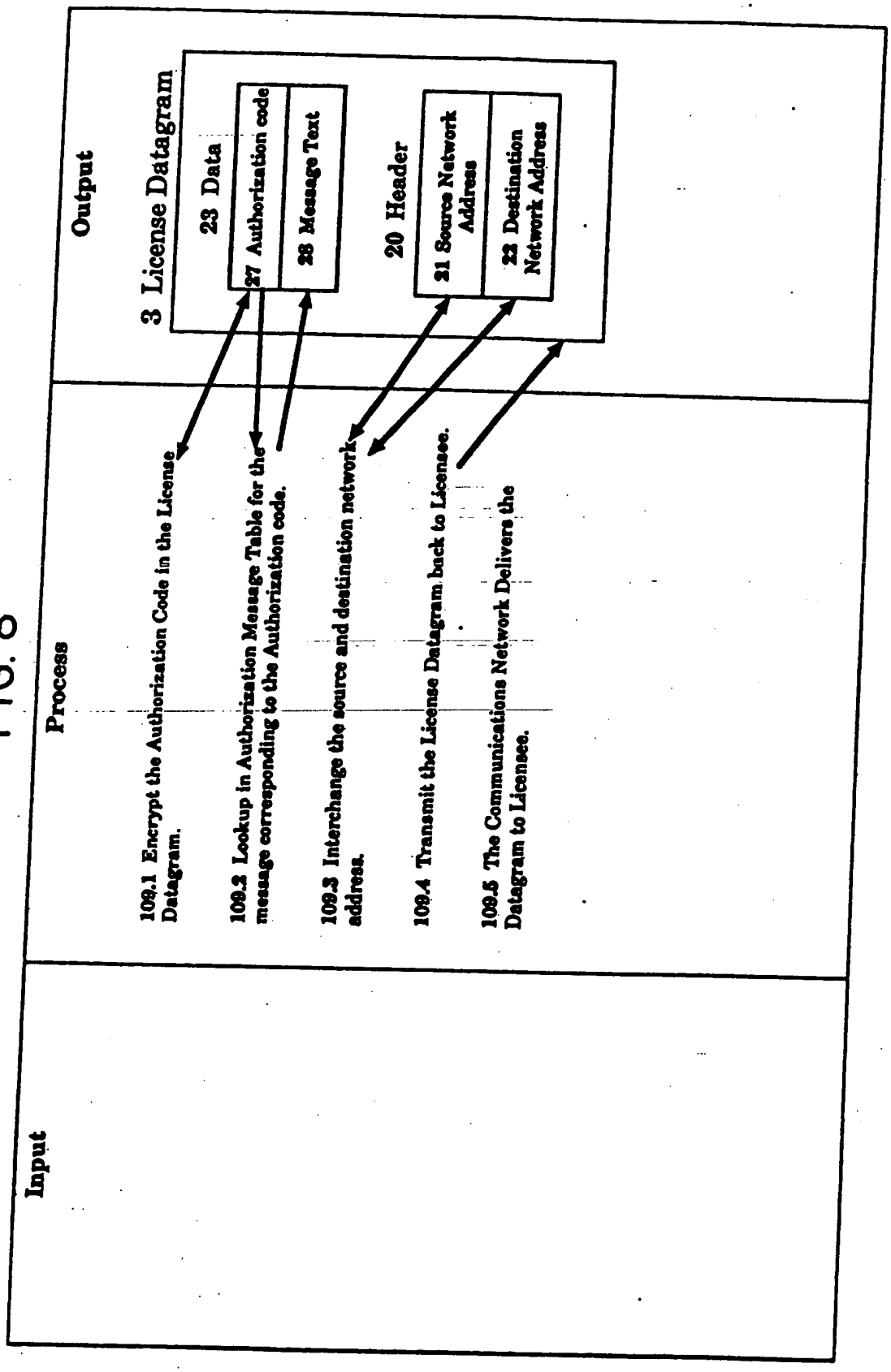

Input
Process
Output
3 License Datagram
23 Data
27 Authorization code
28 Message Text
20 Header
21 Source Network Address
22 Destination Network Address
109.1 Encrypt the Authorization Code in the License Datagram.
109.2 Lookup in Authorization Message Table for the message corresponding to the Authorization code.
109.3 Interchange the source and destination network address.
109.4 Transmit the License Datagram back to Licensee.
109.5 The Communications Network Delivers the Datagram to Licensee.

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US92/05387

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) :G06F 11/34; H04L 9/00
US CL :395/725; 380/4
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/406; 380/25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS DATABASE: Software#, information, usage, monitor?, Licens?

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US,A, 5,103,476 (WAITE ET AL) 07 APRIL 1992 See entire text.	1-110
Y,P	US,A, 5,050,213 (SHEAR) 17 SEPTEMBER 1991 See column 6, lines 27-51.	1-6,9-21,23-26,29-43,45-53,56-59,61-64,67-73,75-110
Y,P	US,A, 5,047,928 (WIEDEMER) 10 SEPTEMBER 1991 See col. 6, lines 16-54.	1-6,9-21,23-36,29-43,45-53,56-59,61-64,67-73,75-110
Y	US,A, 5,023,907 (JOHNSON ET AL) 11 JUNE 1991 See entire document.	1-110

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 AUGUST 1992	04NOV 1992
Name and mailing address of the ISA/ Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. NOT APPLICABLE	Authorized officer Kenneth Williams KENNETH S. KIM Telephone No. (703) 308-1634

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US92/05387

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A, 5,014,234 (EDWARDS, JR.) 07 MAY 1991 See col. 3, lines 4-16.	1-110
Y	US,A, 5,010,571 (KATZNELSON) 23 APRIL 1991 See entire document.	1-6,9-21,23-26,29-43,45-53,56-59,61-64,67-73,75-110.
Y	MACMILLAN Publishing Company, 1985, WILLIAM STALINGS, Data and Computer Communications. p199-203.	1-110
Y,P	US,A, 5,113,519 (JOHNSON ET AL) 12 MAY 1992 See col. 6, lines 36-68.	1-110
Y	US,A, 4,937,863 (ROBERT ET AL) 26 JUNE 1990 See col. 3, lines 25-40.	1-6,9-21,23-26,29-43,45-53,56-59,61-64,67-73,75-110